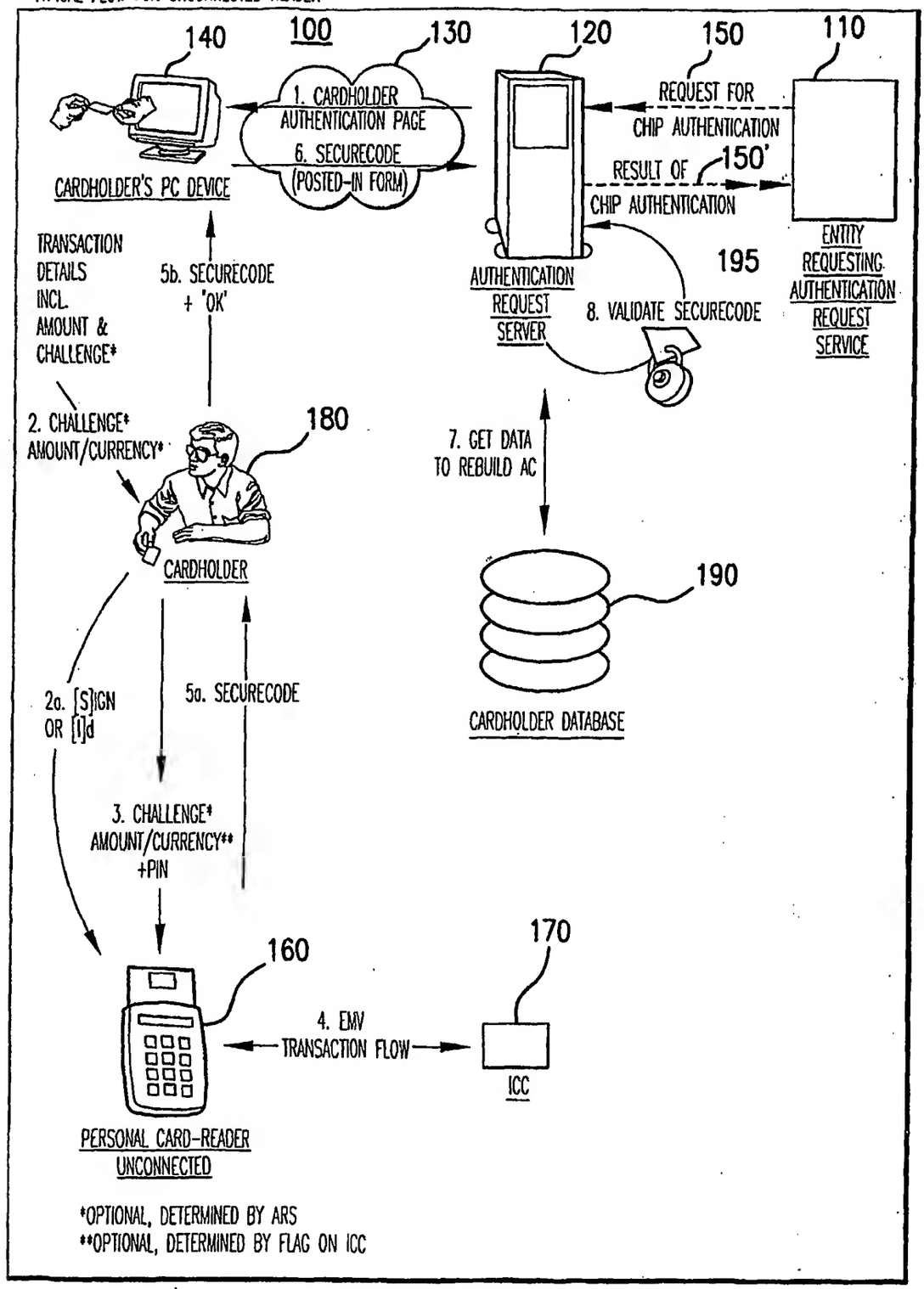
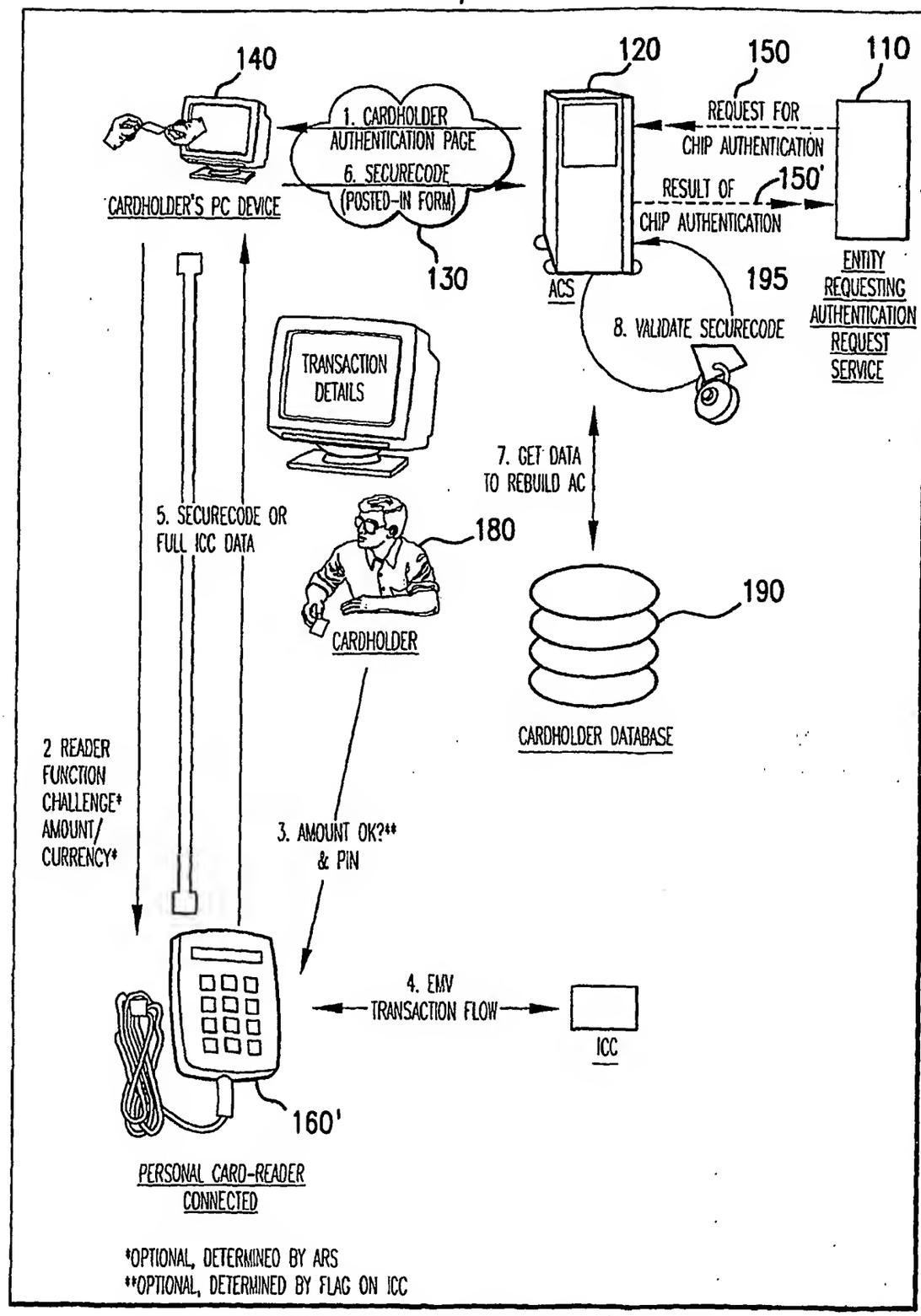


CARDHOLDER AUTHENTICATION USING AN UNCONNECTED READER

FIG. 1



CARDHOLDER AUTHENTICATION USING A CONNECTED READER

FIG.2

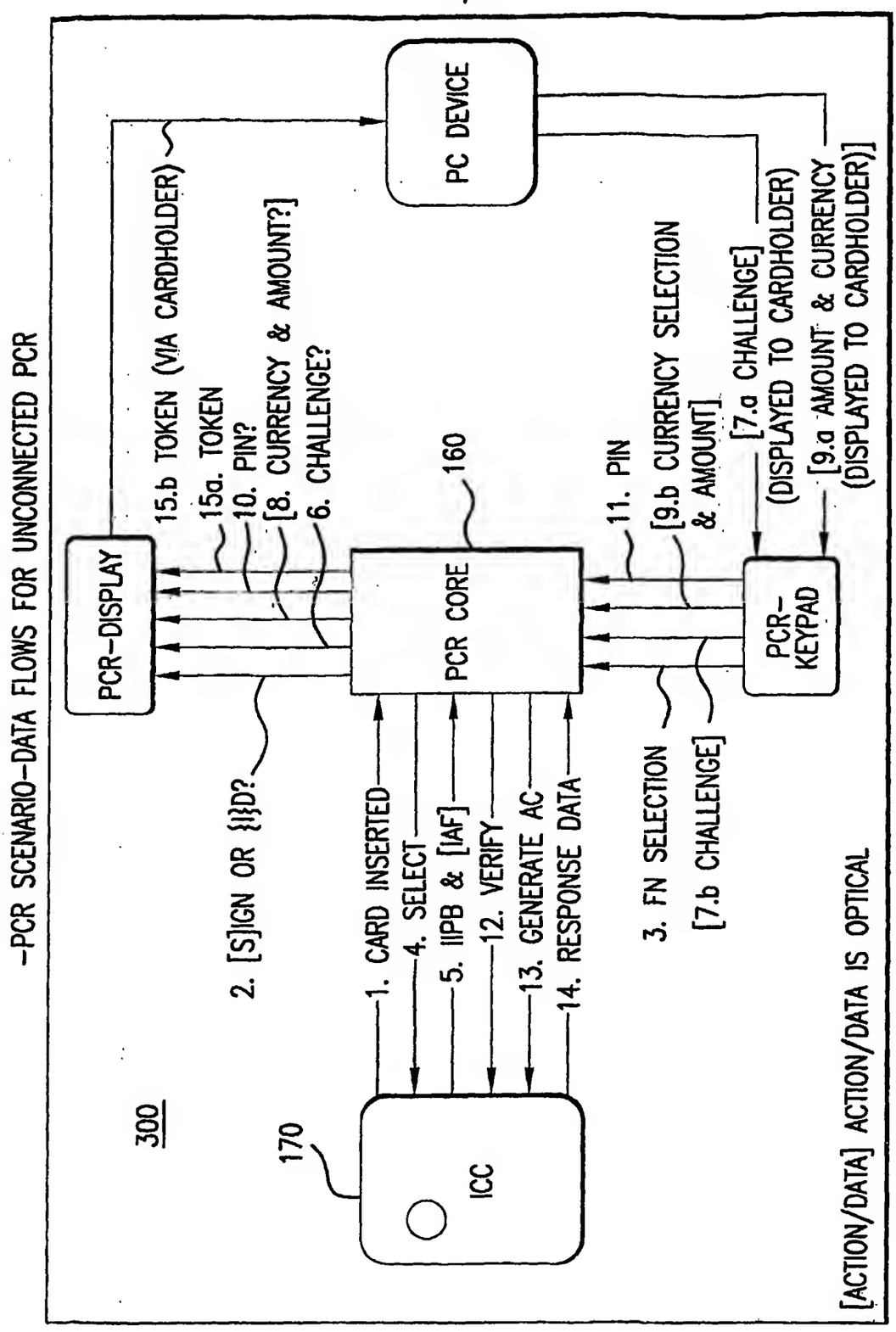

-PCR SCENARIO-DATA FLOWS FOR UNCONNECTED PCR
300
PC DEVICE
PCR-DISPLAY
PCR CORE
160
PCR-KEYPAD
ICC
170
15.b TOKEN (VIA CARDHOLDER)
15a. TOKEN
10. PIN?
[8. CURRENCY & AMOUNT?]
6. CHALLENGE?
2. [S]IGN OR {I}D?
1. CARD INSERTED
4. SELECT
5. IIPB & [IAF]
12. VERIFY
13. GENERATE AC
14. RESPONSE DATA
3. FN SELECTION
[7.b CHALLENGE]
11. PIN
[9.b CURRENCY SELECTION & AMOUNT]
[7.a CHALLENGE] (DISPLAYED TO CARDHOLDER)
[9.a AMOUNT & CURRENCY (DISPLAYED TO CARDHOLDER)]
[ACTION/DATA] ACTION/DATA IS OPTICAL

FIG.3

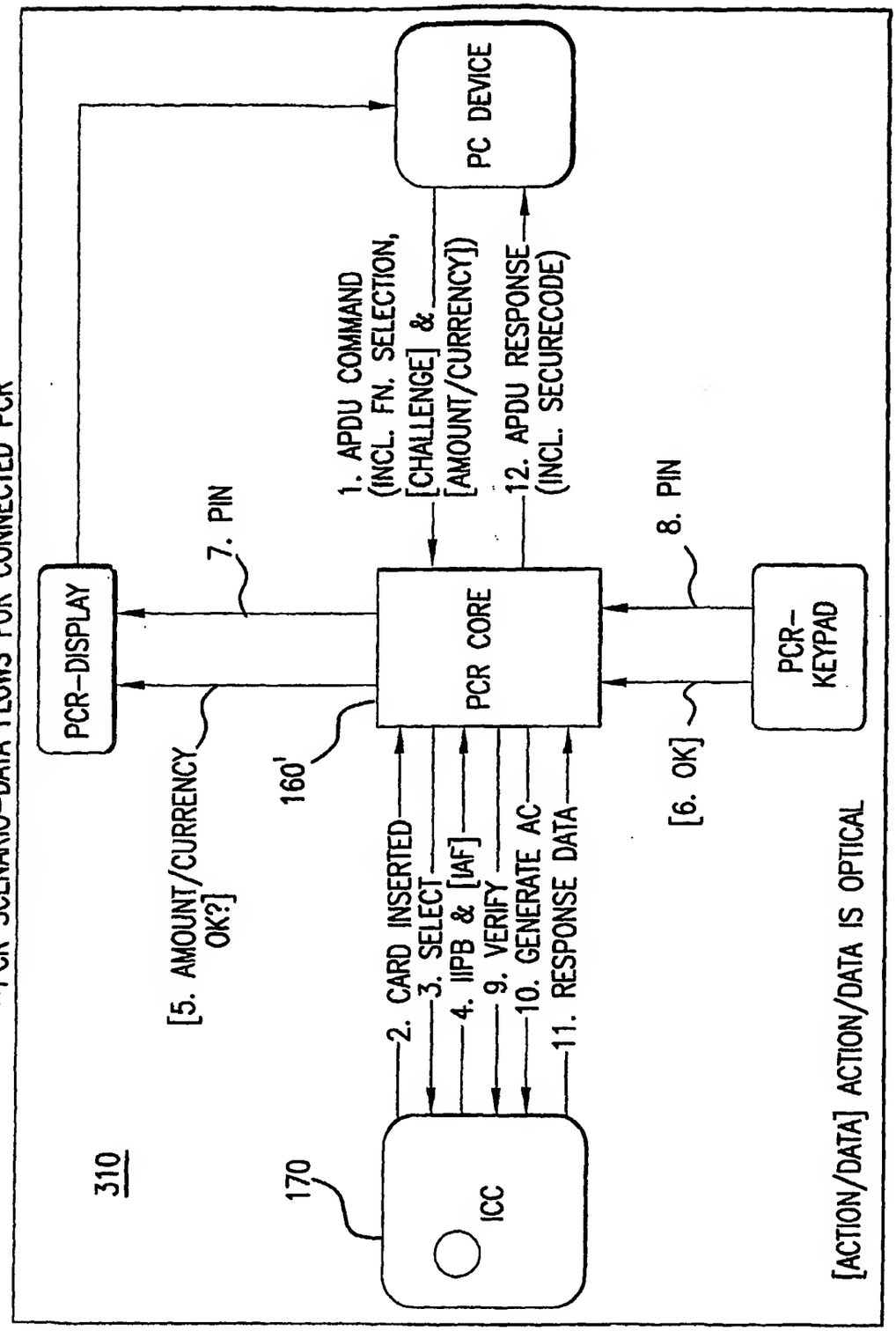

-PCR SCENARIO-DATA FLOWS FOR CONNECTED PCR
PC DEVICE
PCR-DISPLAY
PCR CORE
PCR-KEYPAD
ICC
310
170
160'
1. APDU COMMAND (INCL. FN. SELECTION, [CHALLENGE] & [AMOUNT/CURRENCY])
12. APDU RESPONSE (INCL. SECURECODE)
7. PIN
8. PIN
[5. AMOUNT/CURRENCY OK?]
[6. OK]
2. CARD INSERTED
3. SELECT
4. IIPB & [IAF]
9. VERIFY
10. GENERATE AC
11. RESPONSE DATA
[ACTION/DATA] ACTION/DATA IS OPTICAL

FIG.4

ILLUSTRATION OF EIGHT-DIGIT CHALLENGE AS BCD

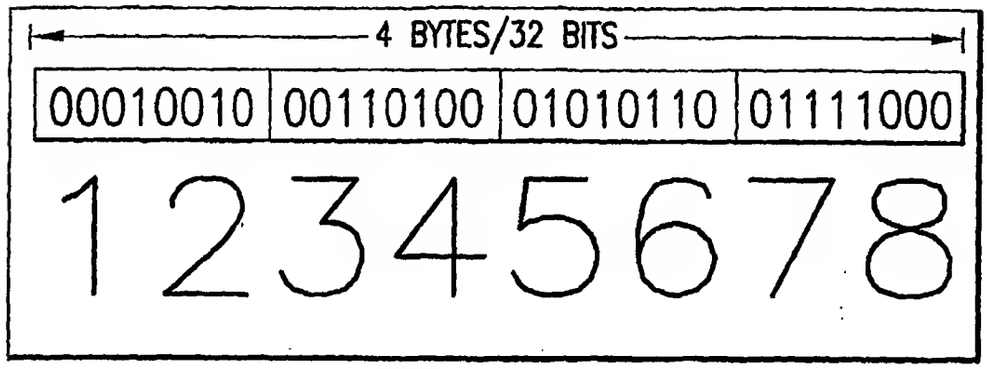


FIG.5

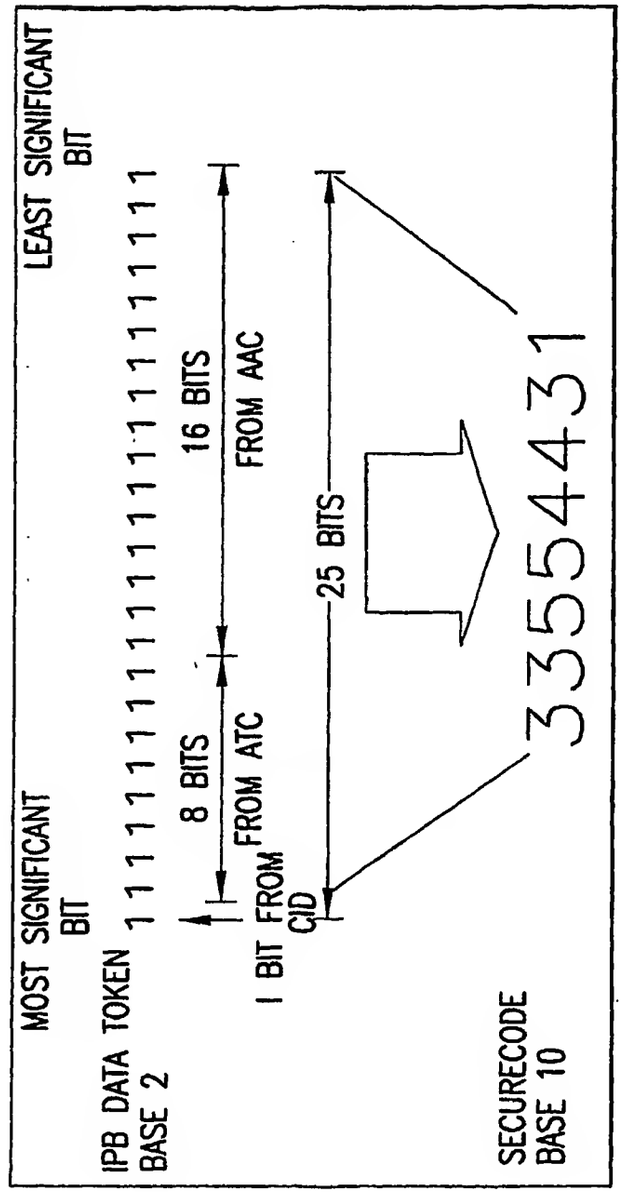

MOST SIGNIFICANT BIT
LEAST SIGNIFICANT BIT
IPB DATA TOKEN BASE 2
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
8 BITS
FROM ATC
1 BIT FROM CID
16 BITS
FROM AAC
25 BITS
SECURECODE BASE 10
33554431

FIG.6

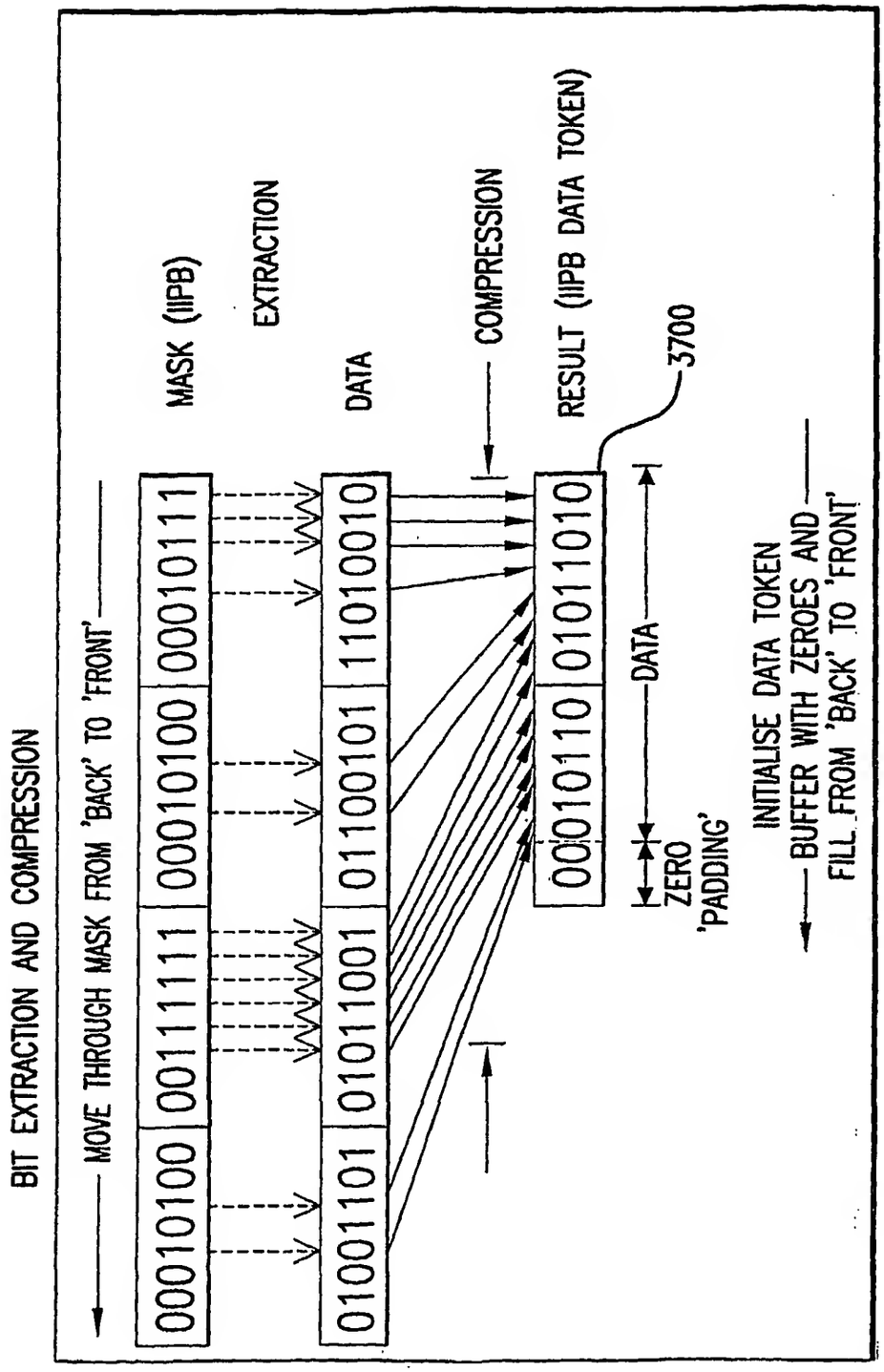

BIT EXTRACTION AND COMPRESSION
MOVE THROUGH MASK FROM 'BACK' TO 'FRONT'
MASK (IIPB)
EXTRACTION
DATA
COMPRESSION
RESULT (IIPB DATA TOKEN)
3700
00010100
00111111
00010100
00010111
01001101
01011001
01100101
11010010
00010110
01011010
DATA
ZERO 'PADDING'
INITIALISE DATA TOKEN BUFFER WITH ZEROES AND FILL FROM 'BACK' TO 'FRONT'

FIG.7

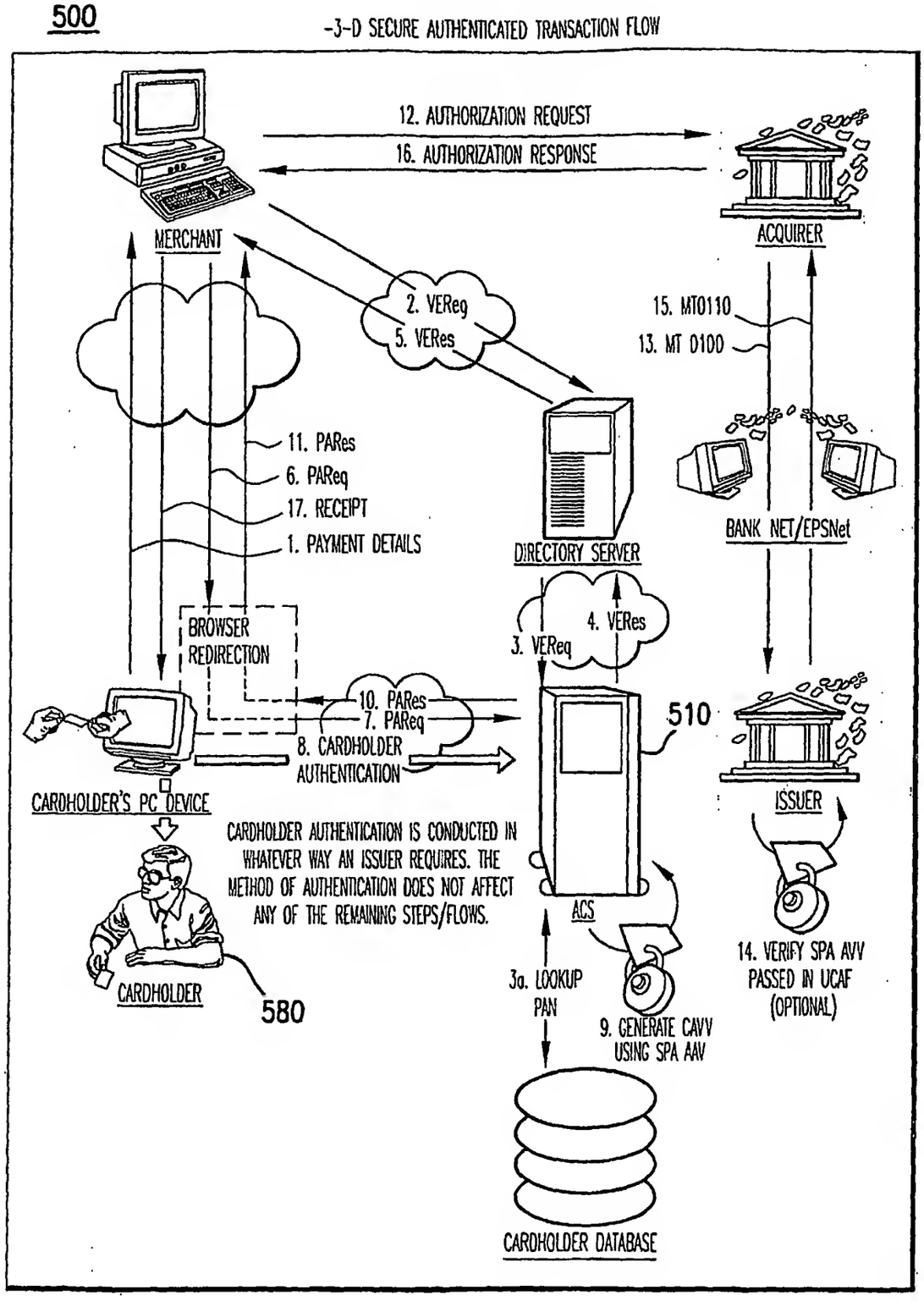

500
-3-D SECURE AUTHENTICATED TRANSACTION FLOW
12. AUTHORIZATION REQUEST
16. AUTHORIZATION RESPONSE
MERCHANT
ACQUIRER
2. VEReq
5. VERes
15. MT0110
13. MT 0100
11. PARes
6. PAReq
17. RECEIPT
1. PAYMENT DETAILS
DIRECTORY SERVER
BANK NET/EPSNet
BROWSER REDIRECTION
4. VERes
3. VEReq
10. PARes
7. PAReq
8. CARDHOLDER AUTHENTICATION
510
CARDHOLDER'S PC DEVICE
ISSUER
CARDHOLDER AUTHENTICATION IS CONDUCTED IN WHATEVER WAY AN ISSUER REQUIRES. THE METHOD OF AUTHENTICATION DOES NOT AFFECT ANY OF THE REMAINING STEPS/FLOWS.
ACS
14. VERIFY SPA AVV PASSED IN UCAF (OPTIONAL)
CARDHOLDER
580
3a. LOOKUP PAN
9. GENERATE CAVV USING SPA AAV
CARDHOLDER DATABASE

FIG.8

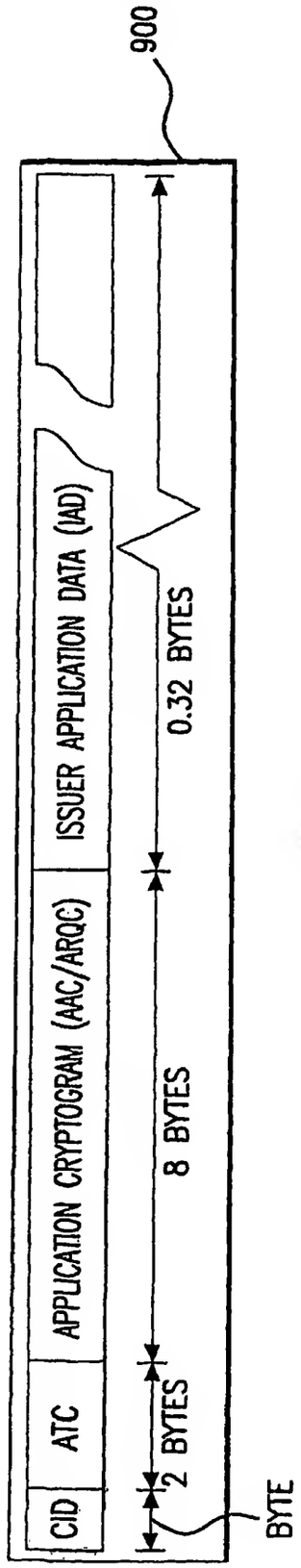

900
CID
ATC
APPLICATION CRYPTOGRAM (AAC/ARQC)
ISSUER APPLICATION DATA (IAD)
1 BYTE
2 BYTES
8 BYTES
0.32 BYTES

FIG.9

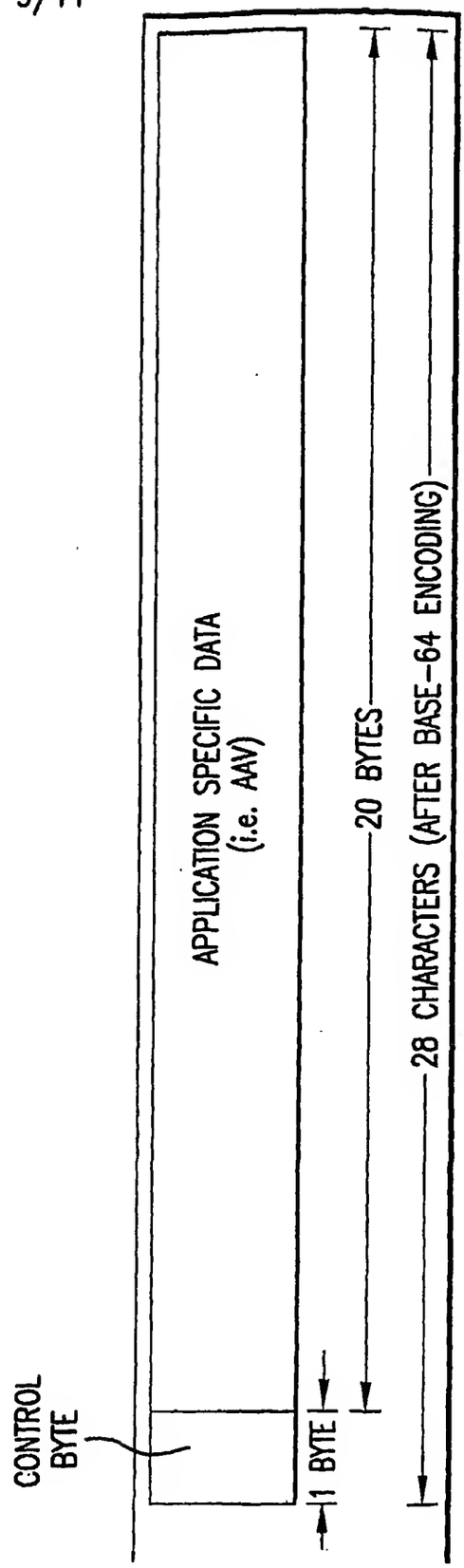

CONTROL BYTE
APPLICATION SPECIFIC DATA (i.e. AAV)
1 BYTE
20 BYTES
28 CHARACTERS (AFTER BASE-64 ENCODING)
UCAF

FIG.10

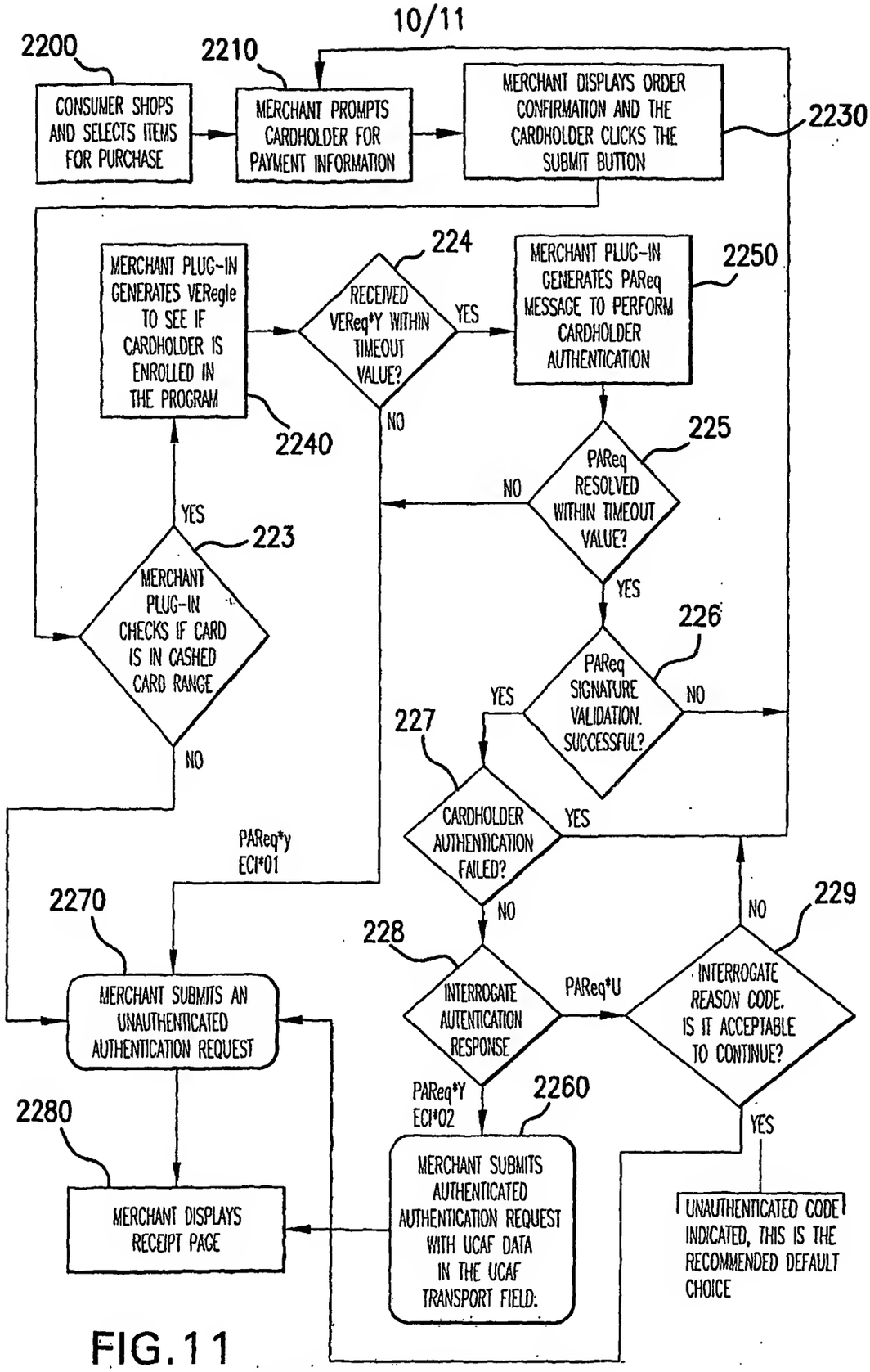

2200
CONSUMER SHOPS AND SELECTS ITEMS FOR PURCHASE
2210
MERCHANT PROMPTS CARDHOLDER FOR PAYMENT INFORMATION
MERCHANT DISPLAYS ORDER CONFIRMATION AND THE CARDHOLDER CLICKS THE SUBMIT BUTTON
2230
MERCHANT PLUG-IN GENERATES VEReqIe TO SEE IF CARDHOLDER IS ENROLLED IN THE PROGRAM
2240
224
RECEIVED VEReq*Y WITHIN TIMEOUT VALUE?
YES
NO
MERCHANT PLUG-IN GENERATES PAReq MESSAGE TO PERFORM CARDHOLDER AUTHENTICATION
2250
225
PAReq RESOLVED WITHIN TIMEOUT VALUE?
NO
YES
223
MERCHANT PLUG-IN CHECKS IF CARD IS IN CASHED CARD RANGE
YES
NO
226
PAReq SIGNATURE VALIDATION SUCCESSFUL?
YES
NO
227
CARDHOLDER AUTHENTICATION FAILED?
YES
NO
PAReq*y
ECI*01
2270
228
INTERROGATE AUTENTICATION RESPONSE
PAReq*U
INTERROGATE REASON CODE. IS IT ACCEPTABLE TO CONTINUE?
NO
229
YES
MERCHANT SUBMITS AN UNAUTHENTICATED AUTHENTICATION REQUEST
PAReq*Y
ECI*02
2260
2280
MERCHANT DISPLAYS RECEIPT PAGE
MERCHANT SUBMITS AUTHENTICATED AUTHENTICATION REQUEST WITH UCAF DATA IN THE UCAF TRANSPORT FIELD.
UNAUTHENTICATED CODE INDICATED, THIS IS THE RECOMMENDED DEFAULT CHOICE

FIG. 11

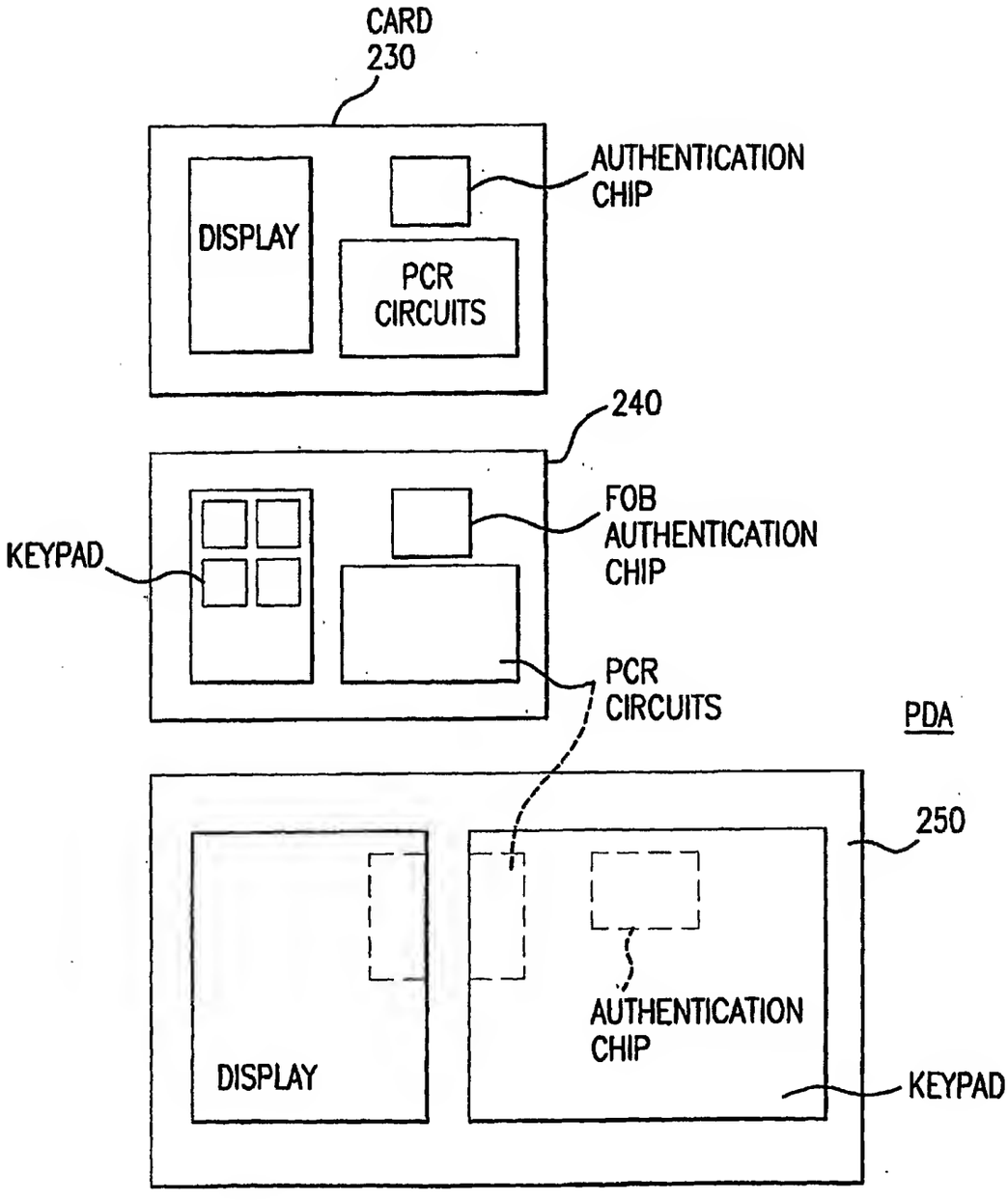

CARD
230
AUTHENTICATION
CHIP
DISPLAY
PCR
CIRCUITS
240
FOB
AUTHENTICATION
CHIP
KEYPAD
PCR
CIRCUITS
PDA
250
AUTHENTICATION
CHIP
DISPLAY
KEYPAD

FIG. 12